NETWORK FORENSICS REPORT

SEPTEMBER 13, 2001

8229 Boone Blvd., Suite 200
Vienna, VA 22-82
Phone: 703.852.0310
Fax: 703.852.0307
Info@forensicsexplorers.com
www.forensicsexplorers.com

This Forensics Explorers audit report of the Montgomery County Public Schools (MCPS) computer network summarizes the traffic assessment, onsite interviews, and survey results performed between June 22, 2001 and September 13, 2001. This report was prepared by the Forensics Explorers Division of CTX Corporation for the Office of Inspector General of Montgomery County with the full cooperation of MCPS.

MCPS COMPUTER NETWORK PROFILE

MCPS employs nearly 20,000 people at over 200 locations including more than 185 school facilities serving over 135,000 students. MCPS operates a large, complex network that provides local computing services and connectivity to the Internet to public schools and administrative offices. Over 4,000 networked computers were active and identified during the audit.

AUDIT SCOPE

This audit was conducted to measure the information security status of the MCPS computer network both where the network connects to the Internet and within the system. Security status was measured against standard and customary practices for perimeter management controls and internally against reasonable expectations of user behavior.

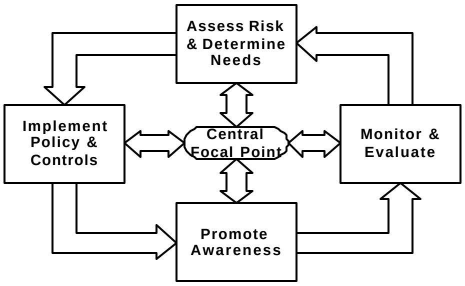
AUDIT METHOD

Forensics Explorers conducted the audit of MCPS computer network from two perspectives: interviews using a standardized survey instrument and network traffic flow reviews using NetWitness™, an enterprise auditing tool. The interviews evaluated management controls and determined customer priorities for the network traffic review. Network monitoring with NetWitness™ allowed auditors to compare MCPS priorities and expectations to actual network activity.

Forensics Explorers conducted interviews with key MCPS personnel to compile baseline information about MCPS network security. The interviews were based on a survey comprised of descriptive questions about the network and staff concerns and Yes/No questions that evaluate the management controls of the organization’s network. Typically, this survey is administered on-site and in person by Forensics Explorers to all computer security staff. We prefer to conduct the survey in person, since many of the questions are subjective and an in-person interview may provide a more complete response. In the case of MCPS, not all potential survey respondents were available while Forensics Explorers was on site. We know that all security personnel did complete the survey and the results of the survey were approved by the MCPS CIO before their return to Forensics Explorers. The survey is in Appendix B.

Forensics Explorers installed two NetWitness™ Collectors on the MCPS network. These collectors allowed Forensics Explorers to audit activity on the network. One NetWitness™ Collector was installed at the gateway between the MCPS network and the Internet. The other was installed on the same segment as the Human Resources Database. This location was chosen based on staff responses to the survey. Staff identified this database as a primary application and security at this location was viewed as critical.

FINDINGS AND RECOMMENDATIONS



Forensics Explorers evaluated MCPS using a Network Risk Assessment Model originally developed by the General Accounting Office. The model examines network security in four areas: (1)Assess Risk & Determine Needs, (2) Implement Policy & Controls, (3) Promote Awareness, and (4) Monitor & Evaluate. These areas are defined as follows:

Assess Risk & Determine Needs – Examines whether an organization has an appreciation of the threats against its networks and has successfully translated these risks into functional requirements.

Implement Policies & Controls – Examines whether an organization has defined policies, procedures, and management controls congruent with priorities identified through the process of risk assessment and needs determination.

Promote Awareness – Examines whether an organization has communicated expectations concerning policies, procedures, and management controls to system users.

Monitor & Evaluate – Examines whether an organization is actively monitoring compliance with its own policies, procedures, and management controls.

ASSESS RISK & DETERMINE NEEDS

1. Recognition of External Threats **Grade: A**

Finding: We found there were procedures in place to review external threats. Each of the security personnel interviewed was quick to point out the need to counter "hacker" threats. In discussions it is clear staff understood the extent and nature of external threats.

Recommendation: We recommend MCPS continue its level of awareness of external threats and review this area yearly.

MCPS Response: *We concur. MCPS is committed to continue this level of awareness of external threats and review yearly.*

2. Recognition of Internal Threats Grade: C

Finding: We found there is insufficient systematic review of the risks posed by inappropriate use by authorized users of the MCPS network. Systematic reviews are conducted on portions of the MCPS network but not across its entirety.

Recommendation: We recommend MCPS review the risks to their business from actions by trusted insiders. Risks should be quantified in terms of probability, impact, and controllability.

MCPS Response: *We concur. In response to the finding: MCPS conducts systematic reviews in areas such as the Human Resources Information System, wide area network use, and mainframe access. For instance, mainframe and Unix administrators systematically examine logs for entries of failed logon attempts and failed attempts to access datasets. On specific scheduled intervals, reports are run to identify and delete retired and terminated staff accounts. Additionally, staff transfer reports are also run regularly and those accounts are disabled until users reapply for more appropriate access. Daily systematic checks are conducted to identify processes running on the system that are unusual. We have increased our capacity to monitor systems by acquiring and implementing software tools that enhance our ability to monitor inappropriate use of the Internet*

In response to the recommendation: We concur that risks should be reviewed and quantified in terms of probability, impact, and controllability. This process has already begun and will be strengthened as new products are implemented.

3. Configuration Control Grade: B+

Finding: We found MCPS had incomplete configuration management controls. MCPS has adequate knowledge of its central and infrastructure configurations; network diagrams were readily available and up-to-date (May 2001). There are some machines not under configuration control and MCPS is working on the remaining machines in accordance with budget constraints. Unauthorized programs present several risks, they use system capacity, and downloaded freeware can contain spyware programs hidden in their code that can allow unauthorized persons access to the MCPS network.

Recommendation: We recommend MCPS complete configuration control over all MCPS systems which do not currently have configuration control. MCPS should maintain a central repository of all users and computers as well as a list of approved software packages. MCPS should have standard desktop images and implement controls to limit unauthorized program installation to simplify management and minimize security threats. Program installation controls could be either technical or administrative.

MCPS Response: *We concur in part. In the school sites, the desktops are standardized and imaged with approved software. In most school sites, desktop management programs such as Novell's ZenWorks are used to prevent unauthorized software installations. In the non-school* *based offices, we are currently working to establish a standard desktop configuration. For example, one third of the desktops that are being replaced this fiscal year will be created using standard desktop images. We are in agreement with the recommendation. Due to budgetary constraints, implementing standardization and desktop asset management systems across the enterprise will be phased in.*

IMPLEMENT POLICIES AND CONTROLS

4. Network Application Patches Grade: C

Finding: We found MCPS does not have automated, enterprise-wide coordinated procedures and systems to ensure that patch levels of externally exposed systems are kept up-to-date. MCPS has successfully protected its networks against threats from the Internet by relying on paper-based logs of patch levels and version releases.

Recommendation: We recommend MCPS define, as part of overall standard operating procedures, a systematic, enterprise-wide schedule for checking exposed systems for known vulnerabilities.

MCPS Response: *We concur. Past practices relied on system administrators keeping paper-based logs of patch levels and version releases. Some system administrators do have procedures in place to ensure that application patches are updated. Although MCPS does not have an enterprise-wide system, systematic reporting of systems and applications will be implemented in May 2002.*

MCPS has procured an enterprise solution that will provide

- *systematic system configuration standards*
- *operational issue analysis*
- *security policy compliance*
- *ensure high performance service levels of mission-critical systems and applications*

Implementation has begun and will be phased in over the next 18 months for all servers in the entire system.

5. User Account Management Grade: C+

Finding: We found MCPS does not have a consistent, enterprise-wide policy for routinely checking for and removing dormant and inactive accounts from the system and checking for expired passwords. Removing dormant accounts and deleting expired passwords limits the avenues for access by former employees and students.

Recommendation: We recommend the Chief Information Officer work with the Chief Operating Officer and the Deputy Superintendent of Schools to improve the information flow between Human Resources and student registration to the Office of Global Access Technology and streamline the processes for creating and deleting users system accounts. Ideally this would be an automated procedure, but a manual process with strong controls would be a useful step to improve control in this area. This control procedure should ensure access is denied to network resources once a student leaves or graduates and an employee leaves MCPS. There should be a routine review of each person's access and employment/educational status and requirements for system access.

MCPS Response: *We concur. The majority of school-based systems have procedures in place to check for dormant and inactive accounts, as well as identifying accounts of students that leave the school during the year. In addition, enterprise systems such as First Class e-mail, Human Resources Information System, and mainframe systems have procedures in place to check for dormant and inactive accounts. However, this is not consistent throughout the entire enterprise.*

Any existing inconsistencies will be eliminated with the implementation of security auditing tools that conduct regular reviews of system user accounts. These tools will provide the ability to systematically identify dormant and inactive accounts, and to enforce password and access policies. Implementation has begun and will be phased in over the next 18 months for all servers in the entire system.

6. Network Security Policies Grade: B

Finding: We found many network security administration policies and procedures in draft rather than final form. It was clear from the security posture that those involved in perimeter defense of the network understood undocumented but in-use procedures designed to protect the perimeter. Proper controls and countermeasures were in place even without formal policies.

Recommendation: We recommend MCPS document these informal policies and procedures and release them to all system administrators and users.

MCPS Response: *We concur. Although the Manual of MCPS Computer Systems Security Procedures is currently in draft, proper controls and countermeasures have long been in place. The document is presently under review by each division in the Office of Global Access Technology and feedback from technical school-based staff will be gathered in February 2002. The document will be finalized and redistributed in March 2002.*

PROMOTE AWARENESS

7. Policies and Procedures Training Grade: C

Finding: We found MCPS does not have a computer security awareness program in place. That is, MCPS does not have a program to communicate and train personnel in its policies and procedures. It is not enough just to have policies and procedures in place, to be effective they must be communicated to users and users must understand the importance of following policies and procedures.

Recommendation: We recommend MCPS formally communicate its policies and procedures to all users and administrators of its networks. MCPS should develop a system to communicate efficiently any new policies or any revisions to current users as soon they are published. We further recommend MCPS document this training with signed agreements which acknowledge receipt of and training in the policies and procedures. This training should be a requirement for all new staff and students before they are given computer access.

MCPS Response: *We concur.*

As a short-term plan, we are implementing the following:

- *The Office of Global Access Technology will feature security in the February 2002 issue of its newsletter, En Touch.*
- *An informational video will be produced in two months. It will cover basic security information such as protecting passwords and how to create a password.*
- *The MCPS security officer has already begun speaking at meetings of MCPS technical support personnel on security topics. One of these meetings included a presentation by Detective Ford of the Montgomery County Police Department.*

The long-range plan includes exploring the following:

- *Implement a system to monitor completion of security training.*
- *Include security awareness as part of new employee orientation.*
- *Ensure security awareness is included as part of technology trainings.*
- *Post information on the MCPS web site and e-mail system.*
- *Include articles in future issues of the MCPS Bulletin and En Touch.*

MONITOR AND EVALUATE

8. Firewall and Perimeter Monitoring Grade: B+

Finding: We found MCPS does not have staff routinely assigned to conduct firewall penetration tests.

Recommendation: We recommend MCPS dedicate specific resources to firewall protection upgrades and conduct periodic penetration testing.

MCPS Response: *We concur. MCPS has procured vulnerability assessment tools to perform security audits. MCPS IT security will conduct periodically scheduled and unscheduled vulnerability tests of the firewall and other network systems.*

9. Incoming Traffic Monitors Grade: C

Finding: We found there are no procedures requiring regular review of audit logs of the monitors on each gateway into the MCPS system. It appears monitors are reviewed, but not necessarily on a systematic basis. Any monitoring and evaluation is conducted at the request of technical support personnel.

Recommendation: We recommend MCPS management require routine monitoring of audit logs.

MCPS Response: *We concur. There are no procedures to regularly review the collected logs of many of the systems making up the MCPS network.*

We have begun routine monitoring of security and system audit logs and will evaluate automated tools to streamline the review process.

10. Outgoing Traffic Monitors Grade: C

Finding: We found MCPS has insufficient monitors in place to evaluate the content of outgoing Internet traffic and traffic between computers within the system. MCPS has adequate security against hacker threats, however these monitors do not evaluate content as related to MCPS policy statements concerning appropriate use. MCPS needs to be aware of inappropriate traffic within and leaving its network as well as inappropriate incoming traffic.

Recommendation: We recommend MCPS management install monitors to ensure compliance with content standards. These monitors should audit all traffic to allow MCPS to periodically review the accuracy of their controls.

MCPS Response: *We concur. MCPS has already taken decisive steps to implement a comprehensive solution.*

11. Improper Traffic Grade: C

Finding: We found evidence of improper traffic on the MCPS network. The improper traffic fell into three categories:

- Malicious Traffic. This type of traffic consists of events intended to deny, disrupt, distort, or destroy MCPS network resources including "hacker" attempts to gain root access to a customer's servers. Malicious activity discovered on the MCPS network, mostly probes from the Internet to web, mail, or dns servers, was lower than expected (0.2 percent of the total traffic collected or about 9 per networked computer compared with unprotected computers on the HoneyNet Project which were attacked 176 times per computer).[1] We do not consider the malicious traffic we observed to be a significant problem because none of the attempts to connect to MCPS resources was successful. However, we did witness an e-mail borne virus reaching a client within MCPS. We were unable to determine if the virus infected the targeted computer.

[1] The HoneyNet Project is a non-profit research group of computer security professionals who analyze network security issues and share proposed solutions.

- Suspicious Traffic. This type of traffic includes activities that defy ready explanation. Either the traffic is unexpected when compared to industry norms for network use or it is unexpected when compared to expected traffic patterns on a customer's system. For example, traffic unique to software that is not known to be in use on the network would be suspicious traffic. We analyzed the contents of suspicious traffic we observed on the MCPS network. Our analysis determined the activities to be peer-to-peer file sharing applications. Peer-to-peer file sharing activities could raise intellectual property concerns and compromise MCPS security through potential viruses, Trojans, and other backdoors imbedded in the shared files.

- Inappropriate Traffic. This type of traffic includes activities that violate customer policy or reasonable standards of behavior. For example, frequent visits to non-work related web sites would be inappropriate traffic. We observed several thousand visits by nearly 100 computers to more than 600 adult web sites and adult chat rooms. The visits constituted 0.12 percent of the web surfing. We also observed downloads of adult materials using peer-to-peer networks; isolated visits to hate- or bias-related web sites; and visits to gambling web sites. Internal users also downloaded and copied songs, movies, and television shows. This inappropriate traffic constitutes a network security risk, an abuse of MCPS property, and a waste of resources.

.

Recommendation: We recommend MCPS install Internet access controls including filters to enforce compliance with a written acceptable use policy. MCPS should institute a program of regular monitoring and make every effort to identify all users engaged in improper traffic. MCPS should appropriately discipline users engaging in all forms of improper traffic.

MCPS Response:

Malicious Traffic*: We concur. MCPS currently has in place a Cisco Pix firewall and a Cisco Secure Intrusion Detection System to monitor and protect against malicious traffic. Although antivirus software was not universally implemented, the software was installed on the majority of enterprise servers and workstations. On January 4, 2002, McAfee Web Shield was implemented to protect the enterprise e-mail traffic. MCPS is in the process of implementing protection for critical systems and network traffic between MCPS and Montgomery County Government.*

Suspicious Traffic*: We concur. In recognizing this vulnerability, MCPS has changed the high-end port availability on the Cisco firewall that has eliminated the use of unauthorized peer-to-peer file sharing applications.*

Inappropriate Traffic*: We concur. MCPS conducted its own internal traffic audit during October and November 2001. The MCPS audit showed that the adult content traffic represented only 0.07 percent of the total Internet traffic. We worked collaboratively with the Inspector General's office, Montgomery County Police, and the MCPS Division of School Safety to review every documented instance of inappropriate use provided in this audit. We have identified specific computers and users involved in this inappropriate use for further action. No criminal* *activity was found. As mentioned before, we have put in place a comprehensive program that not only monitors traffic systematically but we are also working to increase awareness of Regulation IGT-RA so staff and students know the appropriate uses of the school system networked resources. The IT Security Officer is developing enhancements to policies beginning with the previously mentioned Internet filtering work group.*

CONCLUSION

Forensics Explorers thanks staff at Montgomery County Public Schools for their cooperation during this audit. The staff is knowledgeable and has a good understanding of Internet-borne risks and threats. The survey and network observations show MCPS is well postured to address Internet-based “attacks” and unauthorized users. However, MCPS is not well positioned to address internal misuse of the network. MCPS responded appropriately to issues uncovered during the audit. Management is working quickly and diligently to address weaknesses identified in these findings.